REMARKS

Status of the Claims

Claims 8-14 are now present in this application. Claims 8, 11 and 12 are independent.

Claims 8, 11 and 12 have been amended. Reconsideration of this application, as amended, is respectfully requested.

Allowable Subject Matter

The Examiner states that claims 9, 10, 13 and 14 would be allowable if rewritten in independent form. Applicant thanks the Examiner for the early indication of allowable subject matter in this application. Claims 9, 10, 13 and 14 have not been rewritten in independent form at this time, since it is believed that independent claims 8 and 12, from which these claims depend, respectively, are allowable.

Claim Objections

The Examiner has objected to claims 8, 11 and 12 because of informalities. Specifically, the Examiner asserts that the term "capable of" does not constitute a limitation in the patentable sense. Claims 8, 11 and 12 have been amended to replace the term "capable of" with "for" in order to overcome this objection. Reconsideration and withdrawal of this objection are respectfully requested.

Rejection Under 35 U.S.C. § 112, 2nd Paragraph

Claim 8 is rejected under 35 U.S.C. § 112, 2nd Paragraph. This rejection is respectfully traversed.

The Examiner has set forth certain instances wherein the claim language lacks antecedent basis or is not clearly understood. Specifically, the Examiner asserts that in the recitation of "**the** transmission data and **error detection information**", the term "error detection information" lacks antecedent basis.

In order to overcome this rejection, claim 8 has been amended to recite "the transmission data, and error detection information..." for clarification. As amended, the article "the" in "the

transmission data, and error detection information..." only refers to transmission data. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Rejection Under 35 U.S.C. § 102

Claims 8, 11 and 12 are rejected under 35 U.S.C. § 102(b) as being anticipated by Buttler et al. ("Fast, efficient error reconciliation for quantum cryptography", University of California, Los Alamos National Laboratory; hereinafter "Buttler"). This rejection is respectfully traversed.

A complete discussion of the Examiner's rejection is set forth in the Office Action, and is not being repeated here.

Aspects of the present invention improve a quantum key distribution method or apparatus for generating a common key, ensuring security, and correcting a data error using an error correction code.

Independent claim 1 recites, *inter alia*,

> transmission-data estimating including the reception-side communication apparatus **estimating the transmission data** based on a same parity check matrix as that of the transmission-side communication apparatus, the reception data with probability information, the error correction information, and the error detection information; and
>
> encryption-key generating including the transmission-side communication apparatus and the reception-side communication apparatus **discarding a part of the transmission data according to an amount of opened information** and generating an encryption key using rest of the transmission data.

(emphasis added).

Independent claims 11 and 12 recite similar features as part of the above features in claim 1. Thus, it is respectfully submitted that the following remarks also apply to claims 11 and 12.

First, the Examiner cites MPEP 2123, which discusses rejection over prior art's broad disclosure instead of preferred embodiments. The Examiner then concludes that Buttler **generally** teaches and suggests the claimed features.

First, while Applicant understands that MPEP 2123 specifies that nonpreferred and alternative embodiments in a patent reference constitute prior art as stated by the Examiner, the applicability of this portion of MPEP is unclear. Furthermore, the Examiner's statement that

Buttler **generally** teaches and suggests the claimed features does not form any basis for a proper Section 102 rejection. A reference that teaches a **general** concept pertains to the claimed feature is insufficient to establish *prima facie* anticipation.

Instead, in order for a § 102 rejection to be proper, **the cited reference must teach or suggest each and every claimed element**. See M.P.E.P. 2131; M.P.E.P. 706.02. Thus, if the cited reference fails to teach or suggest one or more elements, then the rejection is improper and must be withdrawn. In other words, even assuming, *arguendo*, that Buttler **generally** teaches and suggests the claimed features as asserted, the Examiner still fails to provide a reference that **teaches or suggests each and every claimed element** in order for a § 102 rejection to be proper.

Furthermore, Buttler fails to teach or suggest at least the above-mentioned claimed features in claim 1.

Buttler describes an error reconciliation protocol Winnow based on the exchange for parity and Hamming's "syndrome" for N-bit subunits of a large data set. Specifically, Winnow incorporates a preliminary parity comparison on blocks whose size is $N=2^m$ where $m \in \{3, 4, 5, 6,\ldots\}$. Subsequently, one bit is discarded from these blocks to maintain the privacy of the remaining bits. A Hamming hash function, which can be used to correct single errors, is applied to the remaining N-1 bits on the blocs whose parities did not agree. Finally, m bits are discarded from the blocks on which the Hamming algorithm was applied to maintain the privacy of those bits. As such, Buttler seeks to provide a protocol capable of correcting a higher initial error probability than other protocols. See Abstract and section VII of Buttler.

However, nowhere in Buttler is there any mention or suggestion of a reception-side communication apparatus **estimating the transmission data** based on a same parity check matrix as that of a transmission-side communication apparatus, reception data with probability information, error correction information, and error detection information as claimed. Furthermore, Buttler does not disclose encryption-key generating including the transmission-side communication apparatus and the reception-side communication apparatus **discarding a part of the transmission data according to an amount of opened information** and generating an encryption key using rest of the transmission data as claimed. If this rejection is maintained, Applicant respectfully requests that the Examiner clearly identify prior art that allegedly teaches the claimed features.

Moreover, the Examiner cites general sections of Buttler to support the rejections. However, since the Examiner appears to make interpretations of the applied prior art and claimed features that are not entirely clear to Applicant, in order to have a better understanding of the rejections, Applicant respectfully requests that the Examiner provide specific citations of portions in the applied prior art that allegedly teaches each and every claimed element in a subsequent office action.

In view of the above remarks, it is respectfully submitted that Buttler fails to establish *prima facie* anticipation. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Conclusion

All of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. It is believed that a full and complete response has been made to the outstanding Office Action, and as such, the present application is in condition for allowance.

In view of the above amendment, Applicant believes the pending application is in condition for allowance.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Dennis Powei Chen, Registration No. 61,767 at the telephone number of the undersigned below to conduct an interview in an effort to expedite prosecution in connection with the present application.

If necessary, the Director is hereby authorized in this, concurrent, and future replies to charge any fees required during the pendency of the above-identified application or credit any overpayment to Deposit Account No. 02-2448.

Dated: June 29, 2010

Respectfully submitted,

By _____
D. Richard Anderson
Registration No.: 40439
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Road, Suite 100 East
P.O. Box 747
Falls Church, VA 22040-0747
703-205-8000